REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Objections to Claims

The objections to the claims have been addressed by amending claims 1 and 3 to delete the bullets, by amending claim 1 to add –an– before "exchange" (though "on" has not been deleted for idiomatic reasons), and by amending claim 3 by changing the final comma to a period.

2. Rejection Under 35 USC §112, 2nd Paragraph

This rejection has been addressed by amending claims 1 and 3 to positively recite the objected-to phrases, and by amending claim 3 to delete the "in particular" phraseology.

3. Rejection of Claims 1 and 3-5 Under 35 USC §102(b), and Rejection of Claim 7 Under 35 USC §103(a), in view of "*Smart Card Tutorial - Integrated Circuit Card Standards and Specifications - Part 10*" (Everett)

These rejections are respectfully traversed on the grounds that the Everett publication, like each of the previously applied references, fails to disclose or suggest a chipcard **initialization** step in which:

- parts of respective first and second "values" are respectively generated by the card *and* processing station;
- the processing station determines a secret initial value from at least part of the first value and the transmitted part of the second value; and
- the chip card determines the same secret initial value from at least part of the second value and the transmitted part of the first value, *without the need to actually exchange any part of the secret "initial" value used to initialize the card.*

To the contrary, the Examiner continues to cite publications that are not at all related to the initialization of chip cards, ignoring the positive recitation of chip card initialization. As with so many other documents previously cited by the Examiner, the Everett publication merely describes the method of Diffie-Hellman as it is generally applied when chip cards are used in

terminals, rather than a chip card initialization method, much less a chip card initialization method having the claimed steps.

The Everett publication is directed to use of Diffie-Hellman key exchange in the context of an electronic funds transfer at a point of sale (EFTPOS) terminal using a public connection medium. This is not the same as initialization of a card inserted into a terminal, and the Everett publication does not otherwise disclose any aspect of chip card initialization. Instead of initializing a card inserted into a terminal, which does not involve a public network, Everett is concerned with distribution of keys over a public network. As pointed out in the first paragraph of the text on page 4 of the Everett publication, "*If we consider for example an EFTPOS (Electronic Funds Transfer at the Point Of Sale) scheme it is clear that you can't send a team of people around to every terminal. . ..*" In contrast, the claimed invention concerns precisely the problem of security when a team of people (or at least one person) is in fact sent around to the terminal, and a card inserted into the terminal (it takes a person to insert a card into a terminal). Everett does not consider this problem because Everett assumes that you can't send people around to every terminal. The implication of Everett is that if one did send a person around to every terminal, Diffie-Hellman key exchange would not be needed.

As pointed out in the Appeal Brief, the chip card initialization step, which involves inserting a chip card into a terminal, is not taught in any of the references of record. This includes the Everett publication, which adds nothing to the references already of record, but rather concern "remote" communications (in addition to the above-quoted passage, see the last complete sentence on page 4 of the Everett publication). The prior art simply does not recognize that use of Diffie-Hellman key exchange is needed in the case of a card inserted into a terminal, and therefore could not have anticipated or rendered the concept obvious. In the absence of any teaching or suggestion of a positively recited claim limitation, the rejections of claims 1, 3-5, and 7 under 35 USC §§102(b) and 103(a) are improper and should be withdrawn.

4. Rejection of Claim 2 Under 35 USC §103(a) in view of "*Smart Card Tutorial - Integrated Circuit Card Standards and Specifications - Part 10*" (Everett), "Cryptographic Identification Methods..." (Konigs), and "Handbook of Applied Cryptography" (Menezes)

This rejection is respectfully traversed on the grounds that the Konigs and Menezes articles, like the Everett publication, fail to disclose or suggest a chipcard **initialization** step in which secret initial values are generated both at the card and at the processing station in the manner claimed, by exchange of values used to generate the secret values without actual exchange of any part of the secret initial values.

Instead, as mentioned in the previous response, the Konigs article discloses a method of establishing cryptographic data connections using chipcards without containing any suggestion as to how the chipcards used for the cryptographic data connections are initialized for use in the cryptographic connections, while the Menezes publication merely teaches the use of sequence numbers to identify entities in key establishment protocols, and does not teach any specific initialization method of the type claimed. As a result, withdrawal of the rejection of claim 2 under 35 USC §103(a) is respectfully requested

5. Rejection of Claim 6 Under 35 USC §103(a) in view of "*Smart Card Tutorial - Integrated Circuit Card Standards and Specifications - Part 10*" (Everett) and U.S. Patent No. 5,452,358 (Normile)

This rejection is respectfully traversed on the grounds that the Normile patent, like the the Everett publication, fails to disclose or suggest a chipcard **initialization** step in which secret initial values are generated both at the card and at the processing station in the manner claimed, by exchange of values used to generate the secret values without actual exchange of any part of the secret initial values.

Instead, the Normile patent merely discloses public key encryption of a plaintext message. The public key of a private-public key pair can by definition be exchanged in public, and therefore there is no need to use parallel key generation. The private key, on the other hand, is maintained by only one party, and again there is no need for the claimed type of card

initialization, which is useful for shared-secret key initialization but not for public-private key pair generation.

Because the Normile patent basically has nothing to do with the claimed invention, withdrawal of the rejection of claim 6 under 35 USC §103(a) in view of the Everett publication and the Normile patent is respectfully requested.

6. Rejection of Claim 8 Under 35 USC §103(a) in view of "*Smart Card Tutorial - Integrated Circuit Card Standards and Specifications - Part 10*" (Everett) and U.S. Patent No. 6,038,551 (Barlow)

This rejection is respectfully traversed on the grounds that the Barlow patent, like the Everett publication, fails to disclose or suggest, whether considered individually or in any reasonable combination, a chipcard **initialization** step that does not involve exchange of any part of secret values generated during the initialization.

Instead, the Barlow patent teaches a system that not only exchanges secret keys, but does so by means of public key encryption of the exchanged secret keys. Barlow makes no attempt to only exchange parts of secret values, but rather simply encrypts all of the values before exchange (col. 3, lines 1-13). This public key method of Barlow is not suitable for chipcard initialization of the type claimed, and Barlow does not even remotely suggest a method of generating an initialization value without exchanging the values. To the contrary, whereas the claimed invention is capable of generating initial values for each chipcard manufactured in a relatively simple and yet secure manner, Barlow teaches the difficulty of providing millions of different devices with individual keys, and instead suggests providing them all with a common *public* key. This essentially ***teaches away*** from the claimed invention.

Consequently, withdrawal of the rejection of claim 8 under 35 USC §103(a) in view of the Everett publication and Barlow patent is respectfully requested.

7. Rejection of Claim 9 Under 35 USC §103(a) in view of "*Smart Card Tutorial - Integrated Circuit Card Standards and Specifications - Part 10*" (Everett) and U.S. Patent Nos. 6,038,551 (Barlow) and 5,224,163 (Gasser)

This rejection is again respectfully traversed on the grounds that the Gasser patent, like the Everett publication and Barlow patent, fails to disclose a card **initialization** step in which transfer of data to the card is facilitated by a "secret value" exchange that only involves transfer of "parts" of the respective secret values, and that does not require transformation of the secret values.

Instead, the Gasser patent disclose generation of "session public/private encryption key pairs." The session public/private key pairs are generated, as is common in such session key generating schemes, by mutual exchange and processing of secret values, but there is no disclosure in the Gasser patent that the secret values used in the public/private session key generating process may be transferred to the chipcard by a secret value generated in the manner claimed, using parts of first and second values in the manner claimed.

Accordingly, withdrawal of the rejection of claim 9 under 35 USC §103(a) in view of the Everett publication in view of the Barlow and Gasser patents is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,
BACON & THOMAS, PLLC

Date: July 11, 2006

By: BENJAMIN E. URCIA
Registration No. 33,805

Serial Number 09/492,273

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500